JOINT TESTIMONY OF

DAVID HEYMAN
ASSISTANT SECRETARY FOR POLICY
THE U.S. DEPARTMENT OF HOMELAND SECURITY,

REAR ADMIRAL PAUL F. ZUKUNFT
ASSISTANT COMMANDANT FOR MARINE SAFETY, SECURITY AND STEWARDSHIP
U.S. COAST GUARD, AND

KEVIN K. MCALEENAN
ACTING ASSISTANT COMMISSIONER
OFFICE OF FIELD OPERATIONS
U.S. CUSTOMS AND BORDER PROTECTION

BEFORE

THE HOUSE COMMITTEE ON HOMELAND SECURITY
SUBCOMMITTEE ON BORDER AND MARITIME SECURITY

ON

"BALANCING MARITIME SECURITY AND TRADE FACILITATION: PROTECTING OUR PORTS, INCREASING COMMERCE AND SECURING THE SUPPLY CHAIN"

FEBRUARY 7, 2012

Introduction

Chairwoman Miller, Ranking Member Cuellar and other distinguished Members of the Subcommittee, thank you for the opportunity to appear before the Subcommittee to highlight the Department of Homeland Security's work in the area of supply chain security. This is an issue of singular importance, and we commend the Subcommittee for holding this hearing.

International trade is the engine that powers economies all around the world. Billions of dollars worth of commodities and merchandise move between trading partners every month, by land, by sea, and by air. The modern international trading system—or global supply chain—that undergirds the exchange of goods between countries is a system that has evolved over several decades, built incrementally in an effort to reduce costs and expand markets.

We have experienced a dramatic transformation over the past quarter of a century with the extraordinary integration and interconnection of buyers and suppliers and sellers and manufacturers all over the world. The internet and linkages provided by information and communication technologies has helped to enable this transformation. The end result has been the creation of jobs and wealth and opportunity in areas across the globe.

Today, the global supply chain system provides food, medicine, energy, and myriad of other products that support and sustain our daily lives. This is true around the world. It is a model of economic efficiency built to sustain "just-in-time" delivery, but it also means that our economies are more and more interdependent, one upon each other.

However, the expansive nature of the global supply chain system renders it vulnerable to disruption. Disruptions to the global supply chain can be triggered by a range of causes—manmade or naturally occurring—a number of which we have witnessed in recent years. Whether through terrorist acts like the cargo bomb plot in October 2010 or market-driven forces like the slowdown and lockout in 2002 of twenty nine ports on the West Coast or, most recently, by the volcanic ash clouds of the 2010 eruption of the volcano Eyjafjallajökull in Iceland or the Tsunami that hit Tohoku, Japan in 2011, we see the impact that disruptions can have on our national economies.

Given this, governments and businesses around the world have an interest in transforming the old model of efficiency and adopting a new model based also on ensuring the integrity and reliability of the system as well. In other words, we must move from a model principally focused on "just-in-time" to one also predicated on "just-in-case". It is this notion of a need for greater integrity and reliability that shapes the context for the Administration's new—first ever—strategy to ensure the security and resilience of the global supply chain. It has also been a driving force in our work internationally to foster systems for trade recovery on a global scale.

The Administration's New National Strategy for Global Supply Chain Security

The United States Government, in collaboration with state, local, tribal, international and private sector stakeholders, has undertaken a number of efforts to strengthen the global supply chain.

These efforts include implementation of legislative requirements and a number of strategic efforts with a specific security focus. The Administration's Strategy incorporates and builds upon those prior efforts.

Initially begun in response to a requirement in the Security and Accountability for Every Port (SAFE Port) Act of 2006 that DHS develop a final *Strategy to Enhance International Supply Chain Security* by July, 2010, it was quickly recognized that the multimodal, international nature of the global supply chain system required a broad, all-of-government effort that included input from public and private sector, international and domestic stakeholders. This effort was led by the National Security Staff and is intended to inform and guide efforts by all stakeholders, but especially those of the Federal government.

The focus of the Strategy is the worldwide network of transportation, postal, and shipping pathways, assets, and infrastructure by which goods are moved from the point of manufacture until they reach an end consumer, as well as supporting communications infrastructure and systems. Our approach to supply chain security has two principal goals:

1. To promote the timely and efficient flow of legitimate commerce, while protecting and securing the supply chain from exploitation and reducing its vulnerabilities to disruption; and
2. To foster a global supply chain system that is prepared for and can withstand evolving threats and hazards and can recover rapidly from disruptions.

At its core, the Strategy is about a layered, risk-based and balanced approach in which necessary security measures and resiliency planning are integrated into supply chains. It is about protecting supply chains from being targeted or exploited by those seeking to cause harm. And, it is about maximizing the flow of legitimate commerce. The Strategy achieves this by establishing and adhering to two guiding principles:

1. Galvanize action through a whole-of-government, all-of-Nation approach and by collaborating with state and local governments, the private sector and the international community.
2. Manage risk by utilizing layered defenses, resolving threats as early in the process as possible, and adapting our security posture to changing environments and evolving threats.

Recognizing the good work already accomplished by the United States and the international community, the Strategy does not seek to supplant or impede those efforts. Rather, it seeks to align U.S. and international security and resilience efforts, to foster agile systems able to resolve threats early, improve verification and detection, and reduce systemic vulnerabilities.

The Strategy also sets out eight priority actions upon which immediate implementation efforts will be focused. Through the Strategy, over the next year and beyond, the President has tasked us with:

1. Aligning Federal activities across the U.S. government (USG) to the goals of the Strategy;

2. Refining our understanding of the threats and risks associated with the global supply chain through updated assessments;
3. Advancing technology research, development, testing and evaluation efforts aimed at improving our ability to secure cargo in air, land, and sea environments;
4. Identifying infrastructure projects to serve as models for developing critical infrastructure resiliency best practices;
5. Seeking opportunities to incorporate global supply chain resiliency goals and objectives into Federal infrastructure investment programs and project assessment processes;
6. Promoting necessary legislation to support Strategy implementation by Federal departments and agencies;
7. Developing, in concert with industry and foreign governments, customized solutions to speed the flow of legitimate commerce in specific supply chains that meet designated criteria and can be considered low risk; and
8. Aligning trusted trader program requirements across Federal agencies. We will consider the potential for standardized application procedures, enhanced information-sharing agreements, and security audits conducted by joint or cross-designated Federal teams.

The Strategy also fulfills DHS's SAFE Port Act requirement to submit a *Strategy to Enhance International Supply Chain Security,*' when combined with the DHS report *Fulfilling the SAFE Port Act Requirements*, which was transmitted to this committee on January 25, 2012. This SAFE Port Act requirements report addresses those areas of the Act which Congress directed us to consider, such as impacts to small and medium enterprises and supply chain linkages with terrorism financing. As outlined in the report, we considered these issues carefully and they directly informed the development of the goals and objectives of the Strategy.

Implementation Outreach to Global Supply Chain Stakeholders

Recognizing the interconnected nature of the global supply chain system, the Strategy emphasizes that continued collaboration with global stakeholders is critical.

Over the six months following its release, significant outreach will be conducted by the United States to foreign and domestic stakeholders. We are soliciting their views on how best to implement the Strategy and how best to foster a secure, efficient, and resilient global system.

Outreach to our foreign partners will be accomplished through a collaborative process in which the Department of State and DHS engage with appropriate government Ministries and organizations. This engagement will educate our partners on our strategic goals and objectives and solicit their input of how we can best implement secure, efficient, and resilient systems that span the globe, from the beginnings of supply chains to their end.

We will confer with our domestic partners through a Cross Sector Supply Chain Working Group that DHS has established under the Critical Infrastructure Partnership Advisory Council. Through this process, Critical Infrastructure Sectors will be consulted through their Sector Coordinating Councils (SCC). The general public, or industry segments that do not directly participate in the SCCs, will be able to participate in these discussions as subject matter experts, ensuring we obtain the broadest possible input.

We are specifically interested in receiving views and recommendations from governments, transportation sector partners, and other affected stakeholders on, but not limited to, the following areas:

- Specific opportunities to implement the goals of the *Strategy* and enhance the security, efficiency, and resilience of the global supply chain;
- Understanding evolving threats (man-made as well as natural) and vulnerabilities in the global supply chain as a whole and among different modes of transportation;
- Opportunities to develop or advance international best practices, standards, or guidelines for reducing threats/vulnerabilities and opportunities to encourage global implementation of them;
- Opportunities for the USG to work in concert with industry and the international community to further strengthen the global supply chain, including ways to increase participation in and improve the cost-effectiveness of private-public partnership programs;
- Assumptions that currently inform supply chain security policies and programs that may be incorrect, dated, or obsolete.

The results of the outreach will be combined with other, ongoing work, including threat and risk assessments, to support Federal department and agency implementation planning.

Building on Past and Ongoing Initiatives

While the *National Strategy for Global Supply Chain Security* speaks to our future focus, we would like to address current efforts to secure our ports and waterways and collaborate with our international partners.

GLOBAL INITIATIVES

As discussed previously, we recognized early in the Strategy development process that supply chains are inherently interconnected, intermodal – and global. Even as the Strategy was being created, DHS increased its emphasis on working with the international community to enhance efficiency, security, and resilience and meet the President's strategic goals. Our ongoing efforts now that the Strategy has been released will form a basis for our implementation activities.

In January, 2011, Secretary Napolitano identified global supply chain security as a focal point for our Department.

She specifically emphasized the need for global collaboration – and met with the Secretary Generals of the International Maritime Organization (IMO), the International Civil Aviation Organization (ICAO), and the World Customs Organization (WCO), as well as the leadership of the Universal Postal Union (UPU).

Her engagement has resulted in seven international objectives, which we have been actively pursuing:

1. Identifying and Responding to Evolving Threats/Risks;
2. Expanding Advance Information Requirements Across All Modes;

3. Streamlining “Trusted Trader” Programs;
4. Stemming the Flow of Illicit Shipments of Dangerous Materials;
5. Securing and Facilitating Air Cargo and Global Mail;
6. Building a Resilient System; and
7. Exploring and Deploying New Technologies.

There has been significant progress since January 2011, including not only the practical efforts to improve the security of operations across the global supply chain, but also advancing the institutionalization of these efforts on an international level through new work streams, international bodies committed to our objectives, and new standard-setting processes. Among other results, our work with our partners has had the following impacts:

- The WCO has developed a Risk Management Compendium, enabling Customs administrations to operate under common terminology and criteria to target both high and low risk cargo.
- The ICAO is currently finalizing its Risk Context Statement, which will be presented to the Aviation Security Panel of Experts in March, 2012, creating a common risk definition for aviation security.
- The ICAO established a Transshipment sub-working group to address air cargo that is transshipped through world airports.
- The IMO has completed a user’s guide for *International Ship and Port Facility Security (ISPS) Code* implementation, enhancing compliance and understanding of port security standards.
- The WCO has revised its advance data guidelines, modeled after DHS’s Importer Security Filing rule (better known as “10+2”) and is working on refining air cargo advance data guidelines in coordination with the Air Cargo Advance Screening pilots currently being conducted by DHS.
- DHS has been actively aligning ‘trusted trader’ programs such as the Customs Trade Partnership Against Terrorism (C-TPAT) and the “trusted shipper” concept, and are working with the ICAO and WCO toward creating common global standards.
- The Immigration and Customs Enforcement (ICE) project Global Shield has transitioned into the WCO Program Global Shield, with significantly expanded – and growing – participation across the globe to detect illegal activity and mitigate the misdirection of improvised explosive device precursor materials through seizures and arrests. Under Program Global Shield, more than 89 participating countries are currently sharing information with each other to ensure that chemicals entering their countries are being used in safe and legal ways. As of December 2011, Program Global Shield has accounted for seizures of chemical precursors totaling over 45 metric tons and 19 arrests related to the illicit diversion of these chemicals.
- The International Atomic Energy Agency (IAEA), in collaboration with DNDO, is developing technical standards for detection devices and recommendations on addressing nuclear and other radioactive materials out of regulatory control. DHS is also working

with the IAEA to establish an Action Plan to finalize a list of detection technologies that meet international standards by April, 2012. Based on their analysis, shortfalls in current standards will be identified and targeted for action.

- Work is ongoing with the UPU to strengthen advance information for mail and postal operations and develop a strategy embracing security and advance data sharing measures for consideration at the UPU Congress in October, 2012. The UPU has established emergency contacts in all countries to facilitate the adjudication of potential security alerts and is establishing an international standard for the handling and resolution of anomalies detected at international mail transit hubs.
- The Asia-Pacific Economic Cooperation (APEC) adopted regional information guidelines for government to government and government to private sector communications related to trade recovery in September, 2011. The APEC information guidelines were subsequently adopted by the WCO, creating global guidelines, in December, 2011.

BILATERAL AGREEMENTS AND PARTNERSHIPS

Specific to supply chain security, DHS has entered into Joint Statements or publicly affirmed our mutual commitment through published meeting summaries and statements with a number of nations, and is discussing additional statements with key partners. These statements reaffirm our commitment and our partners' commitments to cooperate, identify key areas of mutual emphasis and principles, and encourage collaboration in our efforts with multilateral forums such as the IMO, ICAO, and WCO. To date, Joint Statements have been signed with New Zealand and the European Commission, and supply chain security has been specifically addressed with the Russian Federation, India, and Canada.

To increase the operational reach of U.S. assets, and to enable partner nation assets to patrol and respond to threats in their own sovereign waters, the U.S. Government has entered into 41 bilateral maritime counter-drug law enforcement agreements. Additionally, the Coast Guard has developed non-binding operational procedures with Mexico, Ecuador, and Peru to facilitate communications between operation centers for the confirmation of registry requests and for permission to stop, board, and search vessels. Coast Guard law enforcement and border security capabilities are evident at both the national and the port level.

The Strategy, and our international agreements and partnerships, also directly support the President's priorities as outlined in the "Beyond the Border" Initiative with Canada and the "21st Century Border Management" Agreement with Mexico. Indeed, many of the specific activities associated with the efforts were informed by and aligned with the strategy during their development.

INTERNATIONAL PORT SECURITY

To address threats farthest from our borders, the Coast Guard establishes and fosters strategic relationships with other nations and international forums. The ISPS Code was created by the IMO with significant Coast Guard assistance. The ISPS Code provides an international regime to ensure ship and port facilities take appropriate preventive measures to ensure security, similar to our domestic regime in the Maritime Transportation Security Act. The International Port Security (IPS) Program sends Coast Guard men and women to foreign ports that conduct maritime trade with the United States to assess the effectiveness of their antiterrorism measures and to verify compliance with ISPS Code. To date, the IPS Program has assessed more than 900 ports and facilities in more than 150 countries.

In 2011, the IPS program assessed the effectiveness of 211 port facilities in 76 of our maritime trading partners. Two countries were found to not have adequate anti-terrorism measures in place in their ports. As a result, they were added to the Coast Guard's Port Security Advisory (PSA) and conditions of entry (COE) were imposed on vessels that have visited one of those ports during their last several port calls before arriving in the United States.

The Coast Guard also supports the European Commission, the Organization of American States, the APEC, and the Secretariat of the Pacific Community to reduce the number of non-compliant foreign ports, thereby reducing and mitigating risk to U.S. ports. Vessels arriving to the United States from non-ISPS compliant countries are required to take additional security precautions, may be boarded by the Coast Guard before being granted permission to enter, and may be refused entry.

As a result of the enactment of the Coast Guard Authorization Act of 2010, the Coast Guard received additional authority to conduct capacity building activities. The Coast Guard has implemented a Port Security Engagement Strategy to expand its engagement with countries beyond minimal ISPS Code implementation to a more robust effort to improve all aspects of port security including legal regimes, maritime domain awareness, and port security operations. The Coast Guard has also developed a Return on Investment Model that identifies countries where capacity building activities would be of the most benefit.

Finally, DHS is pursuing a "Mutual Recognition" Memorandum of Understanding (MOU) with the European Commission (EC). The MOU would call for mutual joint inspections of each other's ports, and the Coast Guard would recognize a successful EC inspection of its Member State's ports the same as a successful country visit by the IPS Program. A similar arrangement is being contemplated with Canada.

MARITIME DOMAIN AWARENESS AND OFFSHORE OPERATIONS

Maritime Domain Awareness (MDA) is a diverse set of capabilities that support all levels (strategic, operational, and tactical) of decision-making. MDA is more than an awareness of ships en route to a particular port; it also entails knowledge of:

- People: Crew, passengers, owners, and operators;
- Cargo: All elements of the global supply chain;
- Infrastructure: Vital elements of the nation's maritime infrastructure, including facilities, services and systems;
- Environment: Weather, environmentally sensitive areas, and living marine resources; and
- Trends: Shipping routes, migration routes and seasonal changes.

Effective MDA requires efficient information sharing that demands coordination among numerous participants at international, Federal, regional, state, local, territorial, and tribal levels of government, as well as with maritime industry and private sector partners.

The Coast Guard's major cutters and deployable forces are critical to the layered security approach. The Coast Guard’s mix of cutters, aircraft, and boats – all operated by highly proficient personnel – allow the Coast Guard to maximize its unique authorities to exercise layered and effective security.

MARITIME INTELLIGENCE AND TARGETING

As the lead DHS agency for maritime homeland security, the Coast Guard screens ships, crews, and passengers for all vessels required to submit a 96-hour Notice of Arrival (NOA) to a U.S. port. CBP’s National Targeting Center (NTC), supported by Coast Guard staff, vets passengers, personnel, and cargo destined for the U.S. Further vetting of the NOA is performed by the Intelligence Coordination Center (ICC), while the two Maritime Intelligence Fusion Centers (MIFCs) focus on screening the vessel itself. The MIFCs associate relevant intelligence and law enforcement analysis to specific vessels, and assess vessel activity. Screening results are passed to the appropriate Coast Guard Sector Command Center, local intelligence staffs, and CBP field offices to be used to ascertain the potential risk posed by a vessel.

AT HOME IN OUR PORTS

Coast Guard Captains of the Port (COTP) are designated as the Federal Maritime Security Coordinator for their port. In this role they lead the Area Maritime Security (AMS) Committees, which often include representatives from CBP, ICE, and the TSA, and oversee the development and regular review of the AMS Plans. AMS Committees have developed strong working relationships with other Federal, state, tribal, territorial, and local law enforcement agencies in an environment that fosters maritime stakeholder participation. Each AMSC reflects the unique challenges and environment of the local port community.

On a national scale, the establishment of Interagency Operations Centers (IOCs) for port security is well underway. Coast Guard, CBP and other agencies are sharing workspace and coordinating operational efforts for improved efficiency and effectiveness of maritime assets in ports including Charleston, Puget Sound, San Diego, Boston and Jacksonville.

The Coast Guard is also responsible for inspecting U.S. port facilities and vessels for safety and security and ensuring compliance with U.S. laws and regulations. In 2011, 10,209 facility safety and security inspections were completed and more than 9,500 Port State Control and Security examinations were conducted on foreign-flag vessels.

CARGO SECURITY and SUPPLY CHAIN INTEGRITY

As the lead DHS agency for cargo security, CBP is at the frontline of protecting the nation from threats, including those posed by containerized cargo. CBP’s security and trade facilitation missions are mutually supportive: by utilizing risk-based strategies, and applying a multilayered approach, CBP can focus time and resources on the small percentage of goods that are high-risk or about which we know the least, which in turn allows CBP to expedite trade that is low-risk or about which we already know a great deal. This approach improves supply chain integrity, promotes economic viability and increases resilience in the event of a disruption to the global supply chain.

CBP's multilayered security approach involves:

- Obtaining information about cargo and those involved in moving it early in the process;
- Using advanced targeting techniques to assess risk and build a knowledge-base about the people and companies involved in the supply chain;
- Fostering partnerships with the private sector and collaborating with other Federal agencies and departments, such as the U.S. Coast Guard, Department of Health and Human Services, the Consumer Product Safety Commission, ICE, and the Department of Agriculture, and with foreign governments, including through information sharing;
- Expanding enforcement efforts to points earlier in the supply chain than simply at our borders; and
- Maintaining robust inspection regimes, including non-intrusive inspection equipment and radiation detection technologies, at our ports of entry.

CBP requires advance electronic cargo information, as mandated in the Trade Act of 2002 (24-Hour Rule, through regulations), for all inbound shipments in all modes of transportation. CBP requires the electronic transmission of additional data, as mandated by the SAFE Port Act, through the Importer Security Filing and Additional Carrier Requirements rule (Security Filing "10+2"), which became effective as an Interim Final Rule on January 26, 2009, and went into full effect on January 26, 2010. Security Filing "10+2" joins the 24 hour rule, and the C-TPAT program and Container Security Initiative (CSI) discussed below, in collecting advance information to improve CBP's targeting efforts.

As part of CBP's layered targeting strategy, the National Targeting Center – Cargo (NTC-C) proactively analyzes advance cargo tactical and strategic information using the Automated Targeting System (ATS) before shipments reach the United States. ATS provides uniform review of cargo shipments for identification of the highest threat shipments, and presents data in a comprehensive, flexible format to address specific intelligence threats and trends. Through targeting rules, the ATS alerts the user to data that meets or exceeds certain predefined criteria. National targeting rule sets have been implemented in ATS to provide threshold targeting for national security risks for all modes of transportation—sea, truck, rail, and air. ATS is a decision support tool for CBP officers working in the NTC-C and in Advanced Targeting Units at our ports of entry and CSI ports abroad allowing officers to focus on the highest threats while facilitating legitimate trade.

NTC-C has established partnerships and liaisons with other agencies, both domestically and abroad. Partnerships with ICE, the Drug Enforcement Administration, the Financial Crimes Enforcement Network (FinCEN), the Department of Commerce, and the Department of Health and Human Services promote information sharing and the exchange of best practices, while collaboration with foreign governments results in seizures and detection of threats at our borders and in foreign ports.

CUSTOMS TRADE PARTNERSHIP AGAINST TERRORISM (C-TPAT)

CBP works with the trade community through the C-TPAT, a voluntary public–private partnership program wherein some members of the trade community adopt tighter security measures throughout their international supply chain and in return are afforded benefits such as reduced exams, front of line examination privileges to the extent possible and practical, and an assigned Supply Chain

Security Specialist who helps them maintain compliance. C-TPAT has enabled CBP to leverage private sector resources to enhance supply chain security and integrity.

CBP conducts records checks on the company in its law enforcement and trade databases and ensures the company meets the security criteria for its particular business sector. Members who pass extensive vetting are certified into the program. Using a risk-based approach, CBP Supply Chain Security Specialists conduct on-site visits of foreign and domestic facilities to confirm that the security practices are in place and operational.

C-TPAT has been a success – membership in this program has grown from 7 companies in its first year to 10,221 as of January 12, 2012. Additionally, CBP is working with foreign partners to establish bi-national recognition and enforcement of C-TPAT. CBP currently has signed mutual recognition arrangements with New Zealand, Canada, Jordan, Japan and Korea and is continuing to work towards similar recognition with the European Union, Singapore, Taiwan and other countries.

CONTAINER SECURITY INITIATIVE (CSI)

Close coordination and joint operations with CBP and ICE in international programs are also critical. The CSI ensures that U.S.-bound maritime containers that pose a high risk are identified and inspected before they are placed on vessels destined for the United States.

Through CSI, CBP stations multidisciplinary teams of officers to work with host country counterparts to identify and examine containers that are determined to pose a high risk for terrorist activity. CSI, the first program of its kind, was announced in January 2002 and is currently operational in 58 foreign seaports—covering more than 80 percent of the maritime containerized cargo shipped to the United States.

CBP officers stationed at CSI ports, with assistance from CSI targeters at the NTC–C, review 100 percent of the manifests originating and/or transiting those foreign ports for containers that are destined for the United States. In this way, CBP identifies and examines high risk containerized maritime cargo prior to lading at a foreign port and before shipment to the United States. In FY 2011, CBP officers stationed at CSI ports reviewed over 9.5 million bills of lading and conducted 45,500 exams in conjunction with their host country counterparts.

CBP is exploring opportunities to utilize emerging technology in some locations, which will allow the program to become more efficient and less costly. In January 2009, CBP began to reduce the number of personnel stationed overseas who perform targeting functions, increasingly shifting more of the targeting of high risk containers to personnel stationed at the NTC–C. This shift in operations reduces costs without diminishing the effectiveness of the CSI program. CSI will become a hybrid of different operational protocols designed around the uniqueness of each foreign port. CBP will remain operational in all 58 locations in fiscal year 2012 with sufficient personnel in country to conduct the examinations of high risk shipments with the host government and to maintain relationships with their host-country counterparts.

SECURE FREIGHT INITIATIVE (SFI)

The SFI partnered with the Department of Energy deploying networks of radiation detection and imaging equipment at six overseas pilot ports. All pilot operations, with the exception of Qasim, Pakistan have ended and those ports have reverted back to the CSI protocols of risk-based targeting. The pilots encountered a number of serious challenges to implementing the 100% scanning mandate.

While each port presented a unique set of challenges, most of the challenges were universal in nature. CBP has documented numerous challenges associated with implementing 100 percent scanning including diplomatic challenges, international trade opposition, the need for port reconfiguration, potential for reciprocal requirements on the United States and lack of available technology to efficiently scan transshipped cargo. It is also important to keep in mind that approximately 80% of the cargo shipped to the United States is sent from only 58 of more than 700 ports. Installing equipment and placing personnel at all of these ports – regardless of volume – would strain government resources without a guarantee of results.

NON INTRUSIVE INSPECTION (NII) / RADIATION DETECTION TECHNOLOGY

The deployment of imaging systems and radiation detection equipment has made a tremendous contribution to CBP's progress in securing the supply chains that bring goods into the United States from around the world against exploitation by terrorist groups. NII technology serves as a force multiplier that allows officers to detect possible anomalies between the contents of a container and the manifest. CBP's use of NII allows us to work smarter and more efficiently in recognizing potential threats and allows cargo to move more expeditiously from the port of entry to the final destination.

CBP has aggressively deployed NII and Radiation Portal Monitor (RPM) technology. Prior to 9/11, only 64 large-scale NII systems, and not a single RPM, were deployed to our country's borders. Today CBP has 301 NII systems and 1388 RPMs. To date, CBP has used the deployed NII systems to conduct over 60 million examinations, resulting in over 11,200 narcotic seizures, with a total weight of over 3.2 million pounds, and more than $45.9 million in undeclared currency seizures. CBP uses RPMs to scan 99 percent of all incoming containerized cargo arriving in the United States by sea and 100% of all passenger and cargo vehicles entering the U.S. land ports of entry. Since RPM program inception in 2002, CBP has scanned over 679 million conveyances for radiological contraband, resulting in more than 2.8 million alarms. CBP's Laboratories and Scientific Services 24/7 Teleforensic Center spectroscopy group at the NTC has responded to nearly 53,000 requests from the field for technical assistance in resolving alarms. To date, 100 percent of alarms have been successfully adjudicated as legitimate trade.

<u>Conclusion</u>

The global supply chain system is an interconnected multimodal system, encompassing foreign and domestic ports, transportation systems, conveyances and infrastructure. Enhancing its security, efficiency, and resilience requires a culture of mutual interest and shared responsibility among stakeholders throughout the world. It requires a balanced approach and the dedication of resources, collaboration – and where necessary, compliance verification and enforcement.

While our efforts to date have been successful, we recognize that further diligence is required. Our new *National Strategy for Global Supply Chain Security* presents a blueprint for change, while building on efforts and infrastructure that have been in place for some time. The risk of natural disasters and other disruptions to the global supply chain presents a risk to our nation's economic strength and vitality. Our Strategy presents an opportunity to continue to promote America's future economic growth and international competitiveness by remaining open and thriving for business.

Thank you again for this opportunity to testify about our efforts.

We look forward to answering any questions you may have.